CROWDSTRIKE University

# SIEM 200:

## Administering and Optimizing Next-Gen SIEM

### Course Overview:

Get hands-on with CrowdStrike Falcon® Next-Gen SIEM in this course designed for system administrators, SIEM administrators, and security tool administrators.

Learn essential skills for administering and optimizing Falcon Next-Gen SIEM. Participants will configure role-based access and manage user/role permissions to establish secure administrative control. Participants will also explore operational best practices, fleet management, and log collector configuration.

### What You Will Learn:

In this course, you will learn how to:

- Navigate and utilize administrative interfaces in the Falcon console
- Configure and manage role-based access control and permissions
- Implement and configure various data ingestion methods and connectors
- Implement event tagging and data segmentation with repositories
- Apply the CrowdStrike Parsing Standard (CPS) and navigate parser management
- Monitor system health and troubleshoot common issues
- Implement administrative best practices

**1-day program | 2 credits**

This instructor-led course includes various walkthrough and hands-on learner exercises.

**Take this class if you are:**
a Falcon platform administrator, Falcon Next-Gen SIEM administrator, security architect, infrastructure support specialist, or security engineer

**Registration:**
For a list of scheduled courses and registration access, please log in to your CrowdStrike University account. This course requires two (2) training credits. If you do not have access to CrowdStrike University, need to purchase training credits, or need more information, please contact sales@crowdstrike.com.

Version: 6.2025

## Recommended Prerequisites

- Fundamental knowledge of SIEM and/or log management platforms
- Ability to comprehend course curriculum presented in English
- Familiarity with Microsoft Windows and Linux system logs
- Recommended courses:
  - **CQL 101:** CrowdStrike Query Language Fundamentals 1
  - **SIEM 100:** Next-Gen SIEM Fundamentals
  - **FALCON 200:** Falcon Platform for Administrators

## Requirements

- Broadband internet connection, web browser, microphone and speakers
- Dual monitors and headset are recommended

## Class Material

Associated materials may be accessed from CrowdStrike University on the day of class.

## Topics

### Falcon Next-Gen SIEM Administration Fundamentals

- Navigate administrative interfaces and locate key configuration areas
- Understand administrator responsibilities
- Identify core administrative components and features
- Practice basic administrative tasks in the console

### Role-Based Access Control

- Create and manage role-based access groups
- Configure search and modification restrictions
- Implement visibility controls
- Develop custom roles with appropriate permissions

### Data Collection and Fleet Management

- Evaluate and implement data collection methods
- Deploy and manage log collectors across the enterprise fleet
- Configure push/pull connectors

## Data Flow Architecture

- Manage event tags and repositories
- Monitor and troubleshoot data flow
- Plan for scalability

## Data Parsing and Parser Management

- Understand parser types and functions
- Navigate parser management
- Troubleshoot parser issues

## System Monitoring and Health

- Track system performance metrics
- Detect and resolve common issues
- Create monitoring dashboards
- Implement health checks


© 2025 CrowdStrike, Inc. All rights reserved.